Using SignaCert with ITIL:

Benefits from an ITIL Perspective

707 SW Washington, 7th Floor
Portland, Oregon 97205
Telephone: 503.227.2207
www.signacert.com

Prepared by Greg Chandler
Sr. Consultant, Pangloss Group, Inc.

Using SignaCert with ITIL:
Benefits from and ITIL Perspective

Introduction

ITIL is a continuously evolving body of knowledge containing good industry practices aimed at integrating IT with business through the formation and management of IT services. Also referred to as IT service management, this philosophy and framework for managing IT services has gained worldwide acceptance as the de-facto standard for IT service management. Implementing ITIL is one way to ensure adherence to emerging regulatory and governance mandates including Sarbanes-Oxley, COBIT, and ISO 20000.

ITIL provides guidance to organizations by describing the processes and functions which are required to support an effective IT service portfolio throughout its lifecycle. While it is not prescriptive, it strongly suggests the use of technology and automation to support these processes. For large enterprises, automation is a requirement of delivering more services at a lower cost.

SignaCert's Enterprise Trust solutions provide automated tools that can greatly benefit companies implementing ITIL processes. SignaCert is an IT compliance solution that measures, catalogs, and reports upon the reality of what's running in your IT production environment against the expected configuration item. This capability benefits those performing the ITIL roles of Configuration Manager, Change Manager, and Release Manager as it is these roles that must ensure what exists in the live environment meets its original intention and purpose.

How SignaCert Benefits ITIL Roles and Processes

The following outlines how SignaCert can be used in real world environments from the perspective of the ITIL processes and roles.

Service Asset and Configuration Management

The goal of the service asset and configuration management (SACM) process is to provide a logical model of the IT infrastructure by identifying, controlling, maintaining and verifying the relationships of the assets and infrastructure which support IT services. Information about each configuration item (CI) including its status and relationship to other CIs is maintained through its lifecycle. This information is housed in a configuration management system (CMS) and is used by numerous other ITIL processes and functions in managing the overall lifecycle of any given IT service. It is one of the most critical processes within the ITIL framework.

The configuration administrator, one of several roles in the SACM process, is responsible for the day to day management of the CMS including the control and receipt of all Configuration Items in the environment. The role also includes managing and maintaining all master copies of software and hardware used in the live environment.

To ensure the CMS matches the live environment and to provide accurate information to other processes, the configuration administrator must regularly audit the infrastructure. In large enterprises this can be a daunting task as there can be thousands of applications supported across multiple IT or business organizations. Accurately identifying which versions of configuration items are in place is nearly impossible given the numerous undocumented changes that occur in most environments.

This is where SignaCert is of great benefit. Using its Global Trust Repository (GTR) of known application, configuration, and system references, it can identify which versions of systems and applications are in use at the application binary or library level. In short, it can identify to the configuration administrator which systems, applications, and modules do not match the reference found in the CMS. Not only does this save hundreds of staff hours in audit research but it can allow the configuration administrator to be proactive in his or her approach to reconcile the variance. This includes working with technical and application management to quickly understand the risks associated with the variance as well as forwarding the information to the Change Manager.

Change Management

Change management is responsible for controlling the lifecycle of all changes and to enable beneficial changes to be made with minimal disruption to IT Services. The change manager authorizes all changes and is ultimately accountable that changes implemented meet their intended purpose.

Given over 80% of incidents are caused by changes made to the infrastructure the process must be rigorous in its evaluation of the change and the change manager must ensure that corporate standards are being used every step of the way. However, because change management can be seen as bureaucratic it is often avoided, especially for small changes. In the urgency to release a new product, patch, or capability many IT employees will implement changes on their own. Because they don't use the change management process, there is no insight into how their change affects others that might be formally introduced in the same period. This often results in unplanned downtime of the IT services provided to the business.

What makes ITIL effective is that all processes are integrated. SignaCert's solution identifies unauthorized changes by detecting the variances between authorized changes, documented in the CMS and what is in the live environment. SignaCert's ability to identify the smallest changes makes it far easier to identify the source of the change and make appropriate remediation. This can serve not only as a watchdog function but one of education as well. The change manager needs to understand why the change management process is avoided to continuously improve the process, or perceptions with it. The easiest way to reduce unplanned downtime is to limit the number of unplanned changes in the environment.

The final step in the change management process is to conduct a post implementation review (PIR). Using SignaCert's reporting the change manager can validate what was deployed, matches what was intended. SignaCert acts as an unbiased, third party to evaluate the change against the reference design giving the Change Manager the confidence to authorize the update to the CMS and establish the new infrastructure baseline.

Release and Deployment Management

This process is responsible for implementing approved changes into the live environment and, among other things, is responsible for:

- Ensuring that each release package consists of a set of related assets and service components that are compatible with each other
- Ensuring that integrity of a release package and its constituent components is maintained throughout the transition activities and recorded accurately in the CMS

Essentially, it is the release and deployment management process which ensures all planned changes are seamlessly introduced into the environment and don't have an impact on the rest of production. This means that for every code change they need to understand compatibility with what is in production. In today's complex application environment, it is hard to fully comprehend how various applications and their modules interact with each other and therefore understand what new introductions might break it.

SignaCert provides the capability for the release management process to understand the relationship and compatibility of applications and code changes before they are deployed. It includes the ability to evaluate against the entire enterprise or just selected applications or servers. For a weekly release of security patches, for example, the release manager can validate which application signatures should be in the live environment and validate the release against those in the test environment. SignaCert provides an added benefit of scanning the production environment to validate what is actually in production. This can avoid many compatibility surprises leading to unplanned downtime and again can help identify unauthorized changes.

Event Management

A new concept in ITIL but one employed by large enterprises for a number of years is event management. An aspect of this process is to detect and escalate exception conditions that have, or may lead, to an Incident. With the output of SignaCert's system integrated with a service desk application, significant events can be detected by the service desk and in many cases proactively dealt with. Dealing with critical systems proactively can avoid unplanned downtime that negatively affects the business.

ISO 20000 - The Next Step

For companies with mature ITIL implementations interested in obtaining ISO 20000 certification, or just to validate the health of their operation, SignaCert can also provide benefit. Until recently, no company could say they are ITIL compliant but growing government and industry regulation have led to a recognized standard in IT Service Management: ISO 20000. ISO 20000 provides a reference of mandatory and recommended specifications, based on ITIL, for any organization offering IT services to internal or external customers. Certification demonstrates that an organization is doing everything mandatory for good service management.

ISO 20000 certification requires the organization to provide evidence that it adheres to the IT Service Management specifications called for in the standard. For example, IT organizations must be able to demonstrate that they have configuration control procedures in place and can demonstrate that the integrity of the systems, services and components are maintained. It also requires that a controlled acceptance test environment shall be established to build and test all releases prior to distribution.

Certification requires an audit by a third party registration body impartial to the outcome but mandatory to obtain certification. Because a third party is involved, the candidate organization must be able to demonstrate, through evidence such as reports, change logs, and other documentation, that they have complied with the specifications called for in the standard.

The reporting capabilities of SignaCert provide evidentiary documentation in areas called for in the standard including information security management and the control processes (configuration and change), and release management. SignaCert's capability to provide a historical view of all changes is a good example of evidence provided to demonstrate adherence to the standard. Because SignaCert can refer to a trusted reference, it demonstrates to the auditor that there are additional controls in place to ensure the integrity of the system configurations.

Summary

SignaCert Enterprise Trust Server used in conjunction with our Global Trust Repository can be implemented as a complementary capability providing benefit to ITIL roles and processes and be of exceptional benefit to those seeking industry ISO 20000 certification. SignaCert Enterprise Trust Server Supports ITIL and Processes:

Service Asset and Configuration Management	Provide continuous compliance audit of the live application environment against the baseline in the Configuration Management System. Detect where the live environment is out of specification.
Change Management	Ensure changes were released to intended configuration. Detect and understand unauthorized changes.

Release and Deployment Management	Ensure Releases will interact properly with the live environment by validating against the provided baseline during testing. Scanning the live environment before release to ensure adherence to application standards.
Event Management	Integrated with a Service Desk application can provide alerts where significant systems or applications are out of sync with the baseline in the CMS. Allows for proactive restoration prior to unplanned downtime.

About Pangloss Group, Inc.

Pangloss Group, Inc. is a Pacific NW based company focused on facilitating measurably improved IT value to the business through adoption of IT Service Management principles based on the ITIL framework. Pangloss provides training, consulting and assessment services to assist the business and IT community in their efforts to integrate IT services with strategic business objectives of the company, academic institution or government agency. They have expertise with current and emerging governance frameworks and standards (i.e. COBIT, Sarbanes-Oxley, ISO 20000).

About SignaCert

SignaCert is the leading provider of next-generation IT compliance solutions allowing organizations to rapidly achieve and prove continuous compliance for the systems that deliver critical business services. SignaCert's patented technology can be quickly deployed and provides immediate visibility into the actual state of IT infrastructure. The SignaCert architecture is designed to seamlessly integrate with existing change processes and continuously monitor critical business services without disruption.

Founded in 2004 by 34-year IT security and compliance industry veteran Wyatt Starnes, SignaCert has assembled a world class team of industry leaders with hands-on IT experience for its executive team, board of directors, and advisory board. SignaCert's customers span a wide variety of industries, including financial services, government, and healthcare.

For more information visit: www.signacert.com.